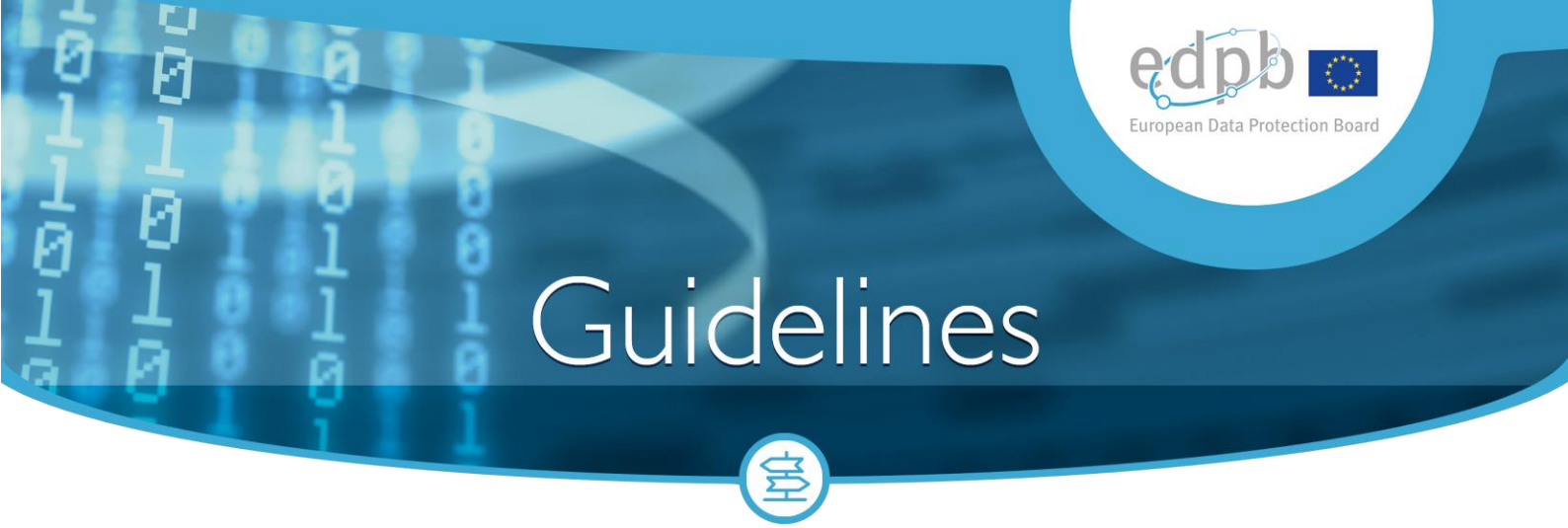

Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)

Version 3.0

4 June 2019

Adopted

Version history

Version 3.0	4 June 2019	Inclusion of Annex 1 (version 2.0 of Annex 1 adopted on 4 June 2019 after public consultation)
Version 2.0	4 December 2018	Adoption of the Guidelines after public consultation - On the same date Annex 1 (version 1.0) was adopted for public consultation
Version 1.0	6 February 2018	Adoption of the Guidelines by the Article 29 Working Party (version for publication consultation). This version has been endorsed by the EDPB on 25 May 2018

Table of Contents

The European Data Protection Board

Having regard to Article 70 (1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,

Having considered the results of the public consultation on the guidelines that took place in February 2018 and on the annex that took place between 14 December 2018 and 1 February 2019, as per Article 70 (4) of the GDPR

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. The General Data Protection Regulation (Regulation (EU) 2016/679) ('the GDPR'), which comes into effect on 25 May 2018, provides a modernised, accountability and fundamental rights based compliance framework for data protection in Europe. A range of measures to facilitate compliance with the provisions of the GDPR are central to this new framework. These include mandatory requirements in specific circumstances (including the appointment of Data Protection Officers and carrying out data protection impact assessments) and voluntary measures such as codes of conduct and certification mechanisms.
2. As part of establishing certification mechanisms and data protection seals and marks, Article 43(1) of the GDPR requires Member States ensure that certification bodies issuing certification under Article 42(1) are accredited by either or both, the competent supervisory authority or the national accreditation body. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied.
3. Meaningful certification mechanisms can enhance compliance with the GDPR and transparency for data subjects and in business to business (B2B) relations, for example between controllers and processors. Data controllers and processors will benefit from an independent third-party attestation for the purpose of demonstrating compliance of their processing operations.[1]
4. In this context, the European Data Protection Board (EDPB)recognizes that it is necessary to provide guidelines in relation to accreditation. The particular value and purpose of accreditation lies in the fact that it provides an authorative statement of the competence of certification bodies that allows the generation of trust in the certification mechanism.

[1] Recital 100 of the GDPR states that the establishment of certification mechanisms can enhance transparency and compliance with the Regulation and allow data subjects to assess the level of data protection of relevant products and services.

5. The aim of the guidelines is to provide guidance on how to interpret and implement the provisions of Article 43 of the GDPR. In particular, they aim to help Member States, supervisory authorities and national accreditation bodies establish a consistent, harmonised baseline for the accreditation of certification bodies that issue certification in accordance with the GDPR.

2 SCOPE OF THE GUIDELINES

6. These guidelines:

- set out the purpose of accreditation in the context of the GDPR;
- explain the routes that are available to accredit certification bodies in accordance with Article 43(1), and identify key issues to consider;
- provide a framework for establishing additional accreditation requirements when the accreditation is handled by the national accreditation body; and
- provide a framework for establishing accreditation requirements, when the accreditation is handled by the supervisory authority.

7. The guidelines do not constitute a procedural manual for the accreditation of certification bodies in accordance with the GDPR. They do not develop a new technical standard for the accreditation of certification bodies for the purposes of the GDPR.

8. The guidelines are addressed to:

- Member States, who must ensure that certification bodies are accredited by the supervisory authority and/or the national accreditation body;
- national accreditation bodies that conduct the accreditation of certification bodies under Article 43(1)(b);
- the competent supervisory authority specifying 'additional requirements' to those in ISO/IEC 17065/2012[2] when the accreditation is carried out by the national accreditation body under Article 43(1)(b);
- the EDPB when issuing an opinion on and approving competent supervisory authority accreditation requirements pursuant to Articles 43(3), 70(1)(p) and 64(1)(c);
- the competent supervisory authority specifying the accreditation requirements when accreditation is carried out by the supervisory authority under Article 43(1)(a);
- other stakeholders such as prospective certification bodies or certification scheme owners providing for certification criteria and procedures[3].

[2] International Organization for Standardization: Conformity assessment -- Requirements for bodies certifying products, processes and services.

[3] Scheme owner is an identifiable organisation which has set up certification criteria and the requirements against which conformity is to be assessed. The accreditation is of the organisation that carries out assessments (Article 43.4) against the certification scheme requirements and issues the certificates (i.e. the certification body, also known as conformity assessment body). The organisation carrying out the assessments could be the same organisation that has developed and owns the scheme, but there could be arrangements where one organisation owns the scheme, and another (or more than one other) performs the assessments.

9. Definitions

10. The following definitions seek to promote a common understanding of the basic elements of the accreditation process. They should be considered as points of reference and they do not raise any claim to be unassailable. These definitions are based on existing regulatory frameworks and standards, especially on the relevant provisions of GDPR and ISO/IEC 17065/2012.

11. For the purposes of these guidelines the following definitions shall apply:

12. '*accreditation*' of certification bodies see section 3 on interpretation of accreditation for the purposes of Article 43 of the GDPR;

13. '*additional requirements*' means the requirements established by the supervisory authority which is competent and against which an accreditation is performed[4];

14. '*certification*' shall mean the assessment and impartial, third party attestation[5] that the fulfilment of certification criteria has been demonstrated;

15. '*certification body*' shall mean a third –party conformity assessment[6] body[7] operating a certification mechanisms[8];

16. '*certification scheme*' shall mean a certification system related to specified products, processes and services to which the same specified requirements, specific rules and procedures apply;[9]

17. 'criteria' or certification criteria shall mean the criteria against which a certification (conformity assessment)is performed;[10]

18. 'national accreditation body' shall mean the sole body in a Member State named in accordance with Regulation (EC) No 765/2008 of the European Parliament and the Council that performs accreditation with authority derived from the State[11].

3 INTERPRETATION OF 'ACCREDITATION' FOR THE PURPOSES OF ARTICLE 43 OF THE GDPR

19. The GDPR does not define 'accreditation'. Article 2 (10) of Regulation (EC) No 765/2008, which lays down general requirements for accreditations, defines accreditation as

[4] Article 43(1), (3) and (6).
[5] Note that according to ISO 17000, third-party attestation (certification) is "applicable to all objects of conformity assessment" (5.5) "except for conformity assessment bodies themselves, to which accreditation is applicable" (5.6).
[6] Third-party conformity assessment activity is performed by an organisation that is independent of the person or organization that provides the object, and of user interests in that object, cf. ISO 17000, 2.4.
[7] See ISO 17000, 2.5: "body that performs conformity assessment services"; ISO 17011: "body that performs conformity assessement services and that can be the object of accreditation"; ISO 17065, 3.12.
[8] Article 42.1, 42.5 GDPR.
[9] See 3.9 in conjuction with Annex B of ISO 17065.

[10] See Article 42(5).
[11] See Article 2.11 765/2008/EC.

20. “an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity “

21. Pursuant to ISO/IEC 17011

22. “accreditation refers to third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks.”

23. Article 43(1) provides:

24. “Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

    (a) the supervisory authority which is competent pursuant to Article 55 or 56;
    (b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council in accordance with ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.”

25. In respect of the GDPR, the accreditation requirements will be guided by:

- ISO/IEC 17065/2012 and the ‘additional requirements’ established by the supervisory authority which is competent in accordance with Article 43 (1)(b), when the accreditation is carried out by the national accreditation body and by the supervisory authority, when it carries out the accreditation itself.

26. In both cases the consolidated requirements must cover the requirements mentioned in Article 43(2).

27. The EDPB acknowledges that the purpose of accreditation is to provide an authoritative statement of the competence of a body to perform certification (conformity assessment activities)[12]. Accreditation in terms of the GDPR shall be understood to mean the following:

28. an attestation[13] by a national accreditation body and/or by a supervisory authority, that a certification body[14] is qualified to carry out certification pursuant to Article 42 and 43 GDPR, taking into account ISO/IEC 17065/2012 and the additional requirements established by the supervisory authority and or by the Board.

[12] Cf. Recital 15 765/2008/EC.
[13] Cf. Article 2.10 Regulation (EC) 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products.
[14] Cf. with the definition of the term “accreditation” pursuant to ISO 17011.

4 ACCREDITATION IN ACCORDANCE WITH ARTICLE 43(1) GDPR

29. Article 43(1) recognises that there are several options for the accreditation of certification bodies. The GDPR requires supervisory authorities and Members States to define the process for the accreditation of certification bodies. This section sets out the routes for accreditation provided in Article 43.

4.1 Role for Member States

30. Article 43(1) requires Member States *to ensure* that certification bodies are accredited, but allows each Member State to determine who should be responsible to conduct the assessment leading to accreditation. On the basis of Article 43(1), three options are available; accreditation is conducted:

(1) solely by the supervisory authority, on the basis of its own requirements;
(2) solely by the national accreditation body named in accordance with Regulation (EC) 765/2008 and on the basis of ISO/IEC 17065/2012 and with additional requirements established by the competent supervisory authority; or
(3) by both the supervisory authority and the national accreditation body (and in accordance with all requirements listed in 2 above).

31. It is for the individual Member State to decide whether the national accreditation body or the supervisory authority or both together will carry out these accreditation activities but in any case it should ensure that adequate resources are provided[15].

4.2 Interaction with Regulation (EC) 765/2008

32. The EDPB notes that Article 2(11) of Regulation (EC) No 765/2008 defines a national accreditation body as "the *sole* body in a Member State that performs accreditation with authority derived from the State".

33. Article 2(11) could be seen as inconsistent with Article 43(1) of the GDPR, which allows accreditation by a body other than the national accreditation body of the Member State. The EDPB considers that the intention of the EU legislation has been to derogate from the general principle that the accreditation be conducted exclusively by the national accreditation authority, by giving supervisory authorities the same power as regards the accreditation of certification bodies. Hence Article 43(1) is lex specialis vis-a-vis Article 2(11) of Regulation 765/2008.

4.3 The role of the national accreditation body

34. Article 43(1)(b) provides that the national accreditation body will accredit certification bodies in accordance with ISO/IEC 17065/2012 and the additional requirements established by the competent supervisory authority.

35. For clarity, the EDPB notes that the specific reference to 'to point (b) of paragraph 1 Article 43(3) implies that 'those requirements' points to the 'additional requirements' established by the competent supervisory authority under Article 43(1)(b) and the requirements set out in Article 43(2).

[15] See Article 4(9) of Regulation (EC) 765/2008.

36. In the process of accreditation, the national accreditation bodies shall apply the additional requirements to be provided by the supervisory authorities.

37. A certification body with existing accreditation on the basis of ISO/IEC 17065/2012 for non-GDPR related certification schemes that wishes to extend the scope of its accreditation to cover certification issued in accordance with the GDPR will need to meet the additional requirements established by the supervisory authority if accreditation is handled by the national accreditation body. If accreditation for certification under the GDPR is only offered by the competent supervisory authority, a certification body applying for accreditation will have to meet the requirements set by the respective supervisory authority.

4.4 The role of the supervisory authority

38. The EDPB notes that Article 57(1)(q) provides that the supervisory authority *shall* conduct the accreditation of a certification body pursuant to Article 43 as a 'supervisory authority task' pursuant to Article 57 and Article 58(3)(e) provides that the supervisory authority has the authorisation and advisory power to accredit certification bodies pursuant to Article 43. The wording of Article 43(1) provides some flexibility and the supervisory authority's accreditation function should be read as a task only where appropriate. Member State law may be used to clarify this point. Yet, in the process of accreditation by a national accreditation body the certification body is required by Article 43(2)(a) to demonstrate their independence and expertise to the satisfaction of the competent supervisory authority in relation to the subject-matter of the certification mechanism it offers.[16]

39. If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not limited to the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides less instruction about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation criteria used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specifiy requirements of ISO 17065. which will contribute to consistency.

40. If a Member State stipulates that the certification bodies are to be accredited by the national accreditation bodies, the supervisory authority should establish additional requirements complementing the existing accreditation conventions envisaged in Regulation (EC) 765/2008 (where Articles 3-14 relate to the organisation and operation of accreditation of conformity assessment bodies) and the technical rules that describe the methods and procedures of the certification bodies. In light of this, Regulation (EC) 765/2008 provides further guidance: Article 2(10) defines accreditation and refers to 'harmonized standards' and 'any additional requirements including those set out in relevant sectoral schemes'. It follows that the additional requirements established by the supervisory authority should include specific requirements and be focused on facilitating the assessment, amongst others, of the independence and level of data protection expertise of certification bodies, for example, their

[16] The additional requirements established by the supervisory authority pursuant to Article 43(1)(b) should specify requirements for independence and expertise. See also Annex 1 of the guidelines.

ability to evaluate and certify personal data processing operations by controllers and processors pursuant to Article 42.(1). This includes competence required for sectoral schemes, and with regard to the protection of fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.[17] The annex to these guidelines can help inform competent supervisory authorities when establishing the 'additional requirements' in accordance with Articles 43(1)(b) and 43(3).

41. Article 43(6) provides that "[t]he requirements referred to in paragraph 3 of this Article and the certification criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form". Therefore, to ensure transparency, all criteria and requirements approved by a supervisory authority shall be published. In terms of quality and trust in the certification bodies, it would be desirable, if all the requirements for accreditation were readily available to the public.

4.5 Supervisory authority acting as certification body

42. Article 42(5) provides that a supervisory authority may issue certifications, but the GDPR does not require it to be accredited to meet the requirements under Regulation (EC) 765/2008. The EDPB notes that Article 43(1)(a) and specifically Article 58(2)(h), 3(a, e-f) empower supervisory authorities to perform both accreditation and certification, and at the same time provide advice, and, where applicable, withdraw certifications, or order certification bodies to not issue certifications.

43. There may be situations where the separation of accreditation and certification roles and duties is appropriate or required, for example, if a supervisory authority and other certification bodies co-exist in a Member State and both issue the same range of certifications. Supervisory authorities should therefore take sufficient organisational measures to separate the tasks under the GDPR to anchor and facilitate certification mechanisms while taking precautions to avoid conflicts of interest that may arise from these tasks. Additionally, Member States and supervisory authorities should keep in mind the harmonised European level when formulating national law and procedures relating to accreditation and certification in accordance with the GDPR.

4.6 Accreditation requirements

44. The annex to these guidelines provides guidance on how to identify additional accreditation requirements. It identifies the relevant provisions in the GDPR and suggests requirements that supervisory authorities and national accreditation bodies should consider to ensure compliance with the GDPR.

45. As established above, where certification bodies are accredited by the national accreditation body pursuant to regulation (EC) 765/2008, ISO/IEC 17065/2012 will be the relevant accreditation standard complemented by the additional requirements established by the supervisory authority. Article 43(2) reflects generic provisions of ISO/IEC 17065/2012 in the light of fundamental rights protection under the GDPR. The framework in the annex uses Article 43(2) and ISO/IEC 17065/2012 as a basis for the identification of requirements plus further criteria relating to the assessment of the data protection expertise of certification bodies and their ability to respect the rights and freedoms of natural persons with respect to the processing of personal data as enshrined in the GDPR. The EDPB notes that it is especially

[17] Article 1(2) GDPR.

focused on ensuring that certification bodies have an appropriate level of data protection expertise in accordance with Article 43(1).

46. The additional accreditation requirements established by the supervisory authority will apply to all certification bodies requesting accreditation. The accreditation body will evaluate whether that certification body is competent to carry out the certification activity in line with the additional requirements and the subject-matter of certification. There shall be references specific sectors or areas of certification for which the certification body is accredited.

47. The EDPB also notes that the special expertise in the field of data protection is also required in addition to ISO/IEC 17065/2012 requirements, if other, external bodies, such as laboratories or auditors, perform parts or components of certification activities on behalf of an accredited certification body. In these cases, accreditation of these external bodies under the GDPR itself is not possible. However, in order to ensure the suitability of these bodies for their activity on behalf of the accredited certification bodies, it is necessary for the accredited certification body to ensure that the data protection expertise required for the accredited body must also be in place and demonstrated with the external body with respect to the relevant activity performed.

48. The framework for identifying the additional accreditation requirements as presented in the annex to these guidelines does not constitute a procedural manual for the accreditation process performed by the national accreditation body or the supervisory authority. It provides guidance on structure and methodology and thus a toolbox to the supervisory authorities to identify the additional requirements for accreditation.

ANNEX 1

Annex 1 provides guidance for the specification of "additional" accreditation requirements with respect to ISO/IEC 17065/2012 and in accordance with Articles 43(1)(b) and 43(3) GDPR.

This Annex sets out suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body or by the competent supervisory authority.[18] These additional requirements are to be communicated to the European Data Protection Board before approval pursuant to Article 64(1)(c).

This Annex should be read in conjunction with ISO/IEC 17065/2012. Section numbers used here correspond to those used in ISO/IEC 17065/2012. Where supervisory authorities perform accreditation pursuant to Article 43(1)(a), good practice would be to follow this approach where practical. This will support EU harmonised accreditation.

Notwithstanding the following guidance or the absence of guidance on any item of ISO/IEC 17065/2012, the competent supervisory authority can formulate further additional requirements concerning these items if in accordance with the national law.

0 PREFIX

[This section is for any agreed Terms of cooperation, if applicable, between the National Accreditation Body and the data protection supervisory authority, e.g. who should be responsible to receive applications or how to organise the acknowledgment of approved criteria as part of the accreditation process.]

1 SCOPE[19]

The scope of ISO/IEC 17065/2012 shall be applied in accordance with the GDPR. The guidelines on accreditation and certification provide further information. The scope of a certification mechanism (for example, certification of cloud service processing operations) should be taken into account in the assessment by the NAB and the competent supervisory authority during the accreditation process, particularly with respect to criteria, expertise and evaluation methodology. The broad scope of ISO/IEC 17065/2012 covering products, processes and services should not lower or override the requirements of the GDPR, e.g. a governance mechanism cannot be the only element of a certification mechanism, as the certification must include processing of personal data, i.e. the processing operations. Pursuant to Article 42(1), GDPR certification is only applicable to the processing operations of controllers and processors.

[18] For information about the approvals process for certification criteria please see section 4 of the certification guidelines.
[19] Numbering refers to ISO/IEC 17065/2012.

2 NORMATIVE REFERENCE

GDPR has precedence over ISO/IEC 17065/2012. If in the additional requirements or by certification mechanism, reference is made to other ISO standards, they shall be interpreted in line with the requirements set out in the GDPR.

3 TERMS AND DEFINITIONS

In the context of this Annex, the terms and definitions of the guidelines on accreditation (WP 261) and certification (EDPB 1/2018) shall apply and have precedence over ISO definitions.

4 GENERAL REQUIREMENTS FOR ACCREDITATION

4.1 Legal and contractual matters

4.1.1 Legal responsibility

A certification body should be able to demonstrate (at all times) to the NAB or CSA that they have up to date procedures that demonstrate compliance with the legal responsibilities set out in the terms of accreditation, including the additional requirements in respect of the application of Regulation 2016/679/EC. Note that, as the certification body is a data controller/processor itself, it shall be able to demonstrate evidence of Regulation 2016/679/EC compliant procedures and measures specifically for controlling and handling of client organisation's personal data as part of the certification process.

The CSA may decide to add further requirements and procedures to check certification bodies GDPR compliance prior to accreditation.

4.1.2 Certification agreement ("CA")

The minimum requirements for a certification agreement shall be supplemented by the following points:

The certification body shall demonstrate in addition to the requirements of ISO/IEC 17065/2012 that its certification agreements:

1. require the applicant to always comply with both the general certification requirements within the meaning of 4.1.2.2 lit. a ISO/IEC 17065/2012 and the criteria approved by the competent supervisory authority or the EDPB in accordance with Article 43 (2)(b) and Article 42(5);
2. require the applicant to allow full transparency to the competent supervisory authority with respect to the certification procedure including contractually confidential matters related to data protection compliance pursuant to Articles 42(7) and 58(1)(c);
3. do not reduce the responsibility of the applicant for compliance with Regulation 2016/679/EC and is without prejudice to the tasks and powers of the supervisory authorities which is competent in line with Article 42(5);
4. require the applicant to provide the certification body with all information and access to its processing activities which are necessary to conduct the certification procedure pursuant to Article 42(6);
5. require the applicant to comply with applicable deadlines and procedures. The certification agreement must stipulate that deadlines and procedures resulting, for

example, from the certification program or other regulations must be observed and adhered to;

6. with respect to 4.1.2.2 lit. c No. 1 ISO/IEC 17065/2012 set out the rules of validity, renewal, and withdrawal pursuant to Articles 42(7) and 43(4) including rules setting appropriate intervals for re-evaluation or review (regularity) in line with Article 42(7);
7. allow the certification body to disclose all information necessary for granting certification pursuant to Articles 42(8) and 43(5);
8. include rules on the necessary precautions for the investigation of complaints within the meaning of 4.1.2.2 lit. c No. 2, additionally, lit. j, shall also contain explicit statements on the structure and the procedure for complaint management in accordance with Article. 43(2)(d);
9. in addition to the minimum requirements referred to in 4.1.2.2 ISO/IEC 17065/2012, if the consequences of withdrawal or suspension of accreditation for the certification body impact on the client, in that case the consequences for the customer should all also be addressed
10. require the applicant to inform the certification body in the event of significant changes in its actual or legal situation and in its products, processes and services concerned by the certification.

4.1.3 Use of data protection seals and marks

Certificates, seals and marks shall only be used in compliance with Article 42 and 43 and the guidelines on accreditation and certification.

4.2 Management of impartiality

The accreditation body shall ensure that in addition to the requirement in 4.2. ISO/IEC 17065/2012

1. the certification body comply with the additional requirements of the competent supervisory authority (pursuant to Article 43(1)(b))
    - **a.** in line with Article 43(2)(a) provide separate evidence of its independence. This applies in particular to evidence concerning the financing of the certification body in so far as it concerns the assurance of impartiality;
    - **b.** its tasks and obligations do not lead to a conflict of interest pursuant to Article 43(2)(e);
2. the certification body has no relevant connection with the customer it assesses.

4.3 Liability and financing

The accreditation body shall in addition to the requirement in 4.3.1 ISO/IEC 17065/2012 ensure on a regular basis that the certification body has appropriate measures (e.g. insurance or reserves) to cover its liabilities in the geographical regions in which it operates.

4.4 Non-discriminatory conditions

Additional requirements may be formulated by the supervisory authority if in accordance with the national law.

4.5 Confidentiality

Additional requirements may be formulated by the supervisory authority if in accordance with the national law.

4.6 Publicly available information

The accreditation body shall in addition to the requirement in 4.6 ISO/IEC 17065/2012 require from the certification body that at minimum

1. all versions (current and previous) of the approved criteria used within the meaning of Article 42(5) are published and easily publicly available as well as all certification procedures, generally stating the respective period of validity;
2. information about complaints handling procedures and appeals are made public pursuant to Article 43(2)(d).

5 STRUCTURAL REQUIREMENTS, ARTICLE 43(4) ["PROPER" ASSESSMENT]

5.1 Organisational structure and top management

Additional requirements may be formulated by the supervisory authority.

5.2 Mechanisms for safeguarding impartiality

Additional requirements may be formulated by the supervisory authority.

6 RESOURCE REQUIREMENTS

6.1 Certification body personnel

The accreditation body shall in addition to the requirement in section 6 ISO/IEC 17065/2012 ensure for each certification body that its personnel:

1. has demonstrated appropriate and ongoing expertise (knowledge and experience) with regard to data protection pursuant to Article 43(1);
2. has independence and ongoing expertise with regard to the object of certification pursuant to Article 43(2)(a) and do not have a conflict of interest pursuant to Article 43(2)(e);
3. undertakes to respect the criteria referred to in Article 42(5) pursuant to Article 43(2)(b);
4. has relevant and appropriate knowledge about and experience in applying data protection legislation;
5. has relevant and appropriate knowledge about and experience in technical and organisational data protection measures as relevant.
6. is able to demonstrate experience in the fields mentioned in the additional requirements 6.1.1, 6.1.4, and 6.1.5, specifically

For personnel with technical expertise:

- Have obtained a qualification in a relevant area of technical expertise to at least EQF[20] level 6 or a recognised protected title (e.g. Dipl. Ing.) in the relevant regulated profession or have significant professional experience.
- *Personnel responsible for certification decisions* require significant professional experience in identifying and implementing data protection measures.

[20] See qualification framework comparison tool at https://ec.europa.eu/ploteus/en/compare?

- *Personnel responsible for evaluations* require professional experience in technical data protection and knowledge and experience in comparable procedure (e.g. certifications/audits), and registered as applicable.

Personnel shall demonstrate they maintain domain specific knowledge in technical and audit skills through continuous professional development.

For personnel with legal expertise:

- Legal studies at a EU or state-recognised university for at least eight semesters including the academic degree Master (LL.M.) or equivalent, or significant professional experience.
- *Personnel responsible for certification decisions* shall demonstrate significant professional experience in data protection law and be registered as required by the Member State.
- *Personnel responsible for evaluations* shall demonstrate at least two years of professional experience in data protection law and knowledge and experience in comparable procedures (e.g. certifications/audits), and when required by the Member State be registered.
    - Personnel shall demonstrate they maintain domain specific knowledge in technical and audit skills through continuous professional development.

6.2 Resources for evaluation

Additional requirements may be formulated by the supervisory authority if in accordance with the national law.

7 PROCESS REQUIREMENTS, ARTICLE 43(2)(C),(D)

7.1 General

The accreditation body shall in addition to the requirement in section 7.1 ISO/IEC 17065/2012 be required to ensure the following:

1. Certification bodies comply with the additional requirements of the competent supervisory authority (pursuant to Article 43(1)(b)) when submitting the application in order that tasks and obligations do not lead to a conflict of interests pursuant to Article 43(2)(b);
2. Notify the relevant CSAs before a certification body starts operating an approved European Data Protection Seal in a new Member State from a satellite office.

7.2 Application

In addition to item 7.2 of ISO/IEC 17065/2012, it should be required that

1. the object of certification (Target of Evaluation, ToE) must be described in detail in the application. This also includes interfaces and transfers to other systems and organizations, protocols and other assurances;
2. the application shall specify whether processors are used, and when processors are the applicant, their responsibilities and tasks shall be described, and the application shall contain the relevant controller/processor contract(s).

7.3 Application Review

In addition to item 7.3 of ISO/IEC 17065/2012, it should be required that

1. binding evaluation methods with respect to the Target of Evaluation (ToE) shall be laid down in the certification agreement;
2. the assessment in 7.3(e) of whether there is sufficient expertise takes into account both technical and legal expertise in data protection to an appropriate extent.

7.4 Evaluation

In addition to item 7.4 of ISO/IEC 17065/2012, certification mechanisms shall describe sufficient evaluation methods for assessing the compliance of the processing operation(s) with the certification criteria, including for example where applicable:

1. a method for assessing the necessity and proportionality of processing operations in relation to their purpose and the data subjects concerned;
2. a method for evaluating the coverage, composition and assessment of all risks considered by controller and processor with regard to the legal consequences pursuant to Articles 30, 32 and 35 and 36 GDPR, and with regard to the definition of technical and organisational measures pursuant to Articles 24, 25 and 32 GDPR, insofar as the aforementioned Articles apply to the object of certification, and
3. a method for assessing the remedies, including guarantees, safeguards and procedures to ensure the protection of personal data in the context of the processing to be attributed to the object of certification and to demonstrate that the legal requirements as set out in the criteria are met; and
4. documentation of methods and findings.

The certification body should be required to ensure that these evaluation methods are standardized and generally applicable. This means that comparable evaluation methods are used for comparable ToEs. Any deviation from this procedure shall be justified by the certification body.

In addition to item 7.4.2 of ISO/IEC 17065/2012, it should be allowed that the evaluation is carried out by external experts who have been recognized by the certification body.

In addition to item 7.4.5 of ISO/IEC 17065/2012, it should be required that data protection certification in accordance with Articles 42 and 43 GDPR, which already covers part of the object of certification, may be included in a current certification. However, it will not be sufficient to completely replace (partial) evaluations. The certification body shall be obliged to check the compliance with the criteria. Recognition shall in any way require the availability of a complete evaluation report or information enabling an evaluation of the previous certification activity and its results. A certification statement or similar certification certificates should not be considered sufficient to replace a report.

In addition to item 7.4.6 of ISO/IEC 17065/2012, it should be required that the certification body shall set out in detail in its certification mechanism how the information required in item 7.4.6 informs the customer (certification applicant) about nonconformities from a certification mechanism. In this context, at least the nature and timing of such information should be defined.

In addition to item 7.4.9 of ISO/IEC 17065/2012, it should be required that documentation be made fully accessible to the data protection supervisory authority upon request.

7.5 Review

In addition to item 7.5 of ISO/IEC 17065/2012, procedures for the granting, regular review and revocation of the respective certifications pursuant to Article 43(2) and 43(3) are required.

7.6 Certification decision

In addition to point 7.6.1 of ISO/IEC 17065/2012, the certification body should be required to set out in detail in its procedures how its independence and responsibility with regard to individual certification decisions are ensured.

7.7 Certification documentation

In addition to item 7.7.1.e of ISO/IEC 17065/2012 and in accordance with Article 42(7) GDPR, it should be required that the period of validity of certifications shall not exceed three years.

In addition to item 7.7.1.e of ISO/IEC 17065/2012, it should be required that the period of the intended monitoring within the meaning of section 7.9 will also be documented.

In addition to item 7.7.1.f of ISO/IEC 17065/2012, the certification body should be required to name the object of certification in the certification documentation (stating the version status or similar characteristics, if applicable).

7.8 Directory of certified products

In addition to item 7.8 of ISO/IEC 17065/2012, the certification body should be required to keep the information on certified products, processes and services available internally and publicly available. The certification body will provide to the public an executive summary of the evaluation report. The aim of this executive summary is to help with transparency around what has been certified and how it was assessed. It will explain such things as:

(a) the scope of the certification and a meaningful description of the object of certification (ToE),

(b) the respective certification criteria (including version or functional status),

(c) the evaluation methods and tests conducted and

(d) the result(s).

In addition to item 7.8 of ISO/IEC 17065/2012 and pursuant to Article 43(5) GDPR, the certification body shall inform the competent supervisory authorities of the reasons for granting or revoking the requested certification.

7.9 Surveillance

In addition to points 7.9.1, 7.9.2 and 7.9.3 of ISO/IEC 17065/2012, and according to Article 43(2)(c) GDPR, it should be required that regular monitoring measures are obligatory to maintain certification during the monitoring period.

7.10 Changes affecting certification

In addition to points 7.10.1 and 7.10.2 of EN ISO/IEC 17065/2012, changes affecting certification to be considered by the certification body shall include: amendments to data protection legislation, the adoption of delegated acts of the European Commission in accordance with Articles 43(8) and 43(9), decisions of the European Data Protection Board and court decisions related to data protection. The change procedures to be agreed here could include such things as: transition periods, approvals process with competent supervisory authority, reassessment of the relevant object of certification and appropriate measures to revoke the certification if the certified processing operation is no longer in compliance with the updated criteria.

7.11 Termination, reduction, suspension or withdrawal of certification

In addition to chapter 7.11.1 of ISO/IEC 17065/2012, the certification body should be required to inform the competent supervisory authority and the NAB where relevant immediately in writing about measures taken and about continuation, restrictions, suspension and withdrawal of certification.

According to Article 58(2)(h), the certification body shall be required to accept decisions and orders from the competent supervisory authority to withdraw or not to issue certification to a customer (applicant) if the requirement for certification are not or no longer met.

7.12 Records

The certification body should be required to keep all documentation complete, comprehensible, up-to-date and fit to audit.

7.13 Complaints and appeals, Article 43(2)(d)

In addition to item 7.13.1 of ISO/IEC 17065/2012, the certification body should be required to define,

(a) who can file complaints or objections,

(b) who processes them on the part of the certification body,

(c) which verifications take place in this context; and

(d) the possibilities for consultation of interested parties.

In addition to item 7.13.2 of ISO/IEC 17065/2012, the certification body should be required to define,

(a) how and to whom such confirmation must be given,

(b) the time limits for this; and

(c) which processes are to be initiated afterwards.

In addition to item 7.13.1 of ISO/IEC 17065/2012, the certification body must define how separation between certification activities and the handling of appeals and complaints is ensured.

8 MANAGEMENT SYSTEM REQUIREMENTS

A general requirement of the management system according to chapter 8 of ISO/IEC 17065/2012 is that the implementation of all requirements from the previous chapters within the scope of the application of the certification mechanism by the accredited certification body is documented, evaluated, controlled and monitored independently.

The basic principle of management is to define a system according to which its goals are set effectively and efficiently, specifically: the implementation of the certification services - by means of suitable specifications. This requires transparency and verifiability of the implementation of the accreditation requirements by the certification body and its permanent compliance.

To this end, the management system must specify a methodology for achieving and controlling these requirements in compliance with data protection regulations and for continuously checking them with the accredited body itself.

These management principles and their documented implementation must be transparent and be disclosed by the accredited certification body pursuant in the accreditation procedure pursuant to Article 58 and thereafter at the request of the data protection supervisory authority at any time during an investigation in the form of data protection reviews pursuant to Art. 58(1)(b) or a review of the certifications issued in accordance with Article 42(7) pursuant to Article 58(1)(c).

In particular, the accredited certification body must make public permanently and continuously which certifications were carried out on which basis (or certification mechanisms or schemes), how long the certifications are valid under which framework and conditions (recital 100).

8.1 General management system requirements

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.2 Management system documentation

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.3 Control of documents

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.4 Control of records

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.5 Management Review

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.6 Internal audits

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.7 Corrective actions

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.8 Preventive actions

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

9 FURTHER ADDITIONAL REQUIREMENTS21

9.1 Updating of evaluation methods

The certification body shall establish procedures to guide the updating of evaluation methods for application in the context of the evaluation under point 7.4. The update must take place in the course of changes in the legal framework, the relevant risk(s), the state of the art and the implementation costs of technical and organisational measures.

9.2 Maintaining expertise

Certification bodies shall establish procedures to ensure the training of their employees with a view to updating their skills, taking into account the developments listed in point 9.1.

9.3 Responsibilities and competencies

[21] The competent supervisory authority may specify and add further additional requirements if in accordance with national law.

9.3.1 Communication between CB and its customers

Procedures shall be in place for implementing appropriate procedures and communication structures between the certification body and its customer. This shall include

1. Maintaining documentation of tasks and responsibilities by the accredited certification body, for the purpose of
    a. Information requests, or
    b. To enable contact in the event of a complaint about a certification.
2. Maintaining an application process for the purpose of
    a. Information on the status of an application;
    b. Evaluations by the competent supervisory authority with respect to
        i. Feedback;
        ii. Decisions by the competent supervisory authority.

9.3.2 Documentation of evaluation activities

Additional requirements may be formulated by the supervisory authority.

9.3.3 Management of complaint handling

A complaint handling shall be established as an integral part of the management system, which shall in particular implement the requirements of points 4.1.2.2 lit. c), 4.1.2.2 lit. j), 4.6 lit. d) and 7.13 ISO/IEC 17065/2012.

Relevant complaint and objections should be shared with the competent supervisory authority.

9.3.4 Management of withdrawal

The procedures in the event of suspension or withdrawal of the accreditation shall be integrated into the management system of the certification body including notifications of customers.